AMENDMENTS TO THE SPECIFICATION

Please amend the application by rewriting the paragraphs in the specification with the following clean paragraphs in accordance with 37 CFR § 1.121; a marked-up set of the paragraphs are included in the following section.

Paragraph at page 31, lines 5-20:

Continuing with the configuration phase, client SSO manager **510** uses the public key belonging to user **500** to obtain or generate an attribute certificate in the following manner. Client SSO manager **510** encrypts one or more sets of authentication data **512** with the public key of user **500**, thereby generating encrypted authorization attributes **526**. The encrypted authorization information is then placed into request **528** for requesting an attribute certificate, along with associated identifying information for user **500** and target legacy applications **502** as required by the format of the request and/or attribute certificate, and sent to attribute certificate authority **529**. In the preferred embodiment, the encrypted authorization information has been generated with an appropriate format so that attribute certificate authority **529** can copy it into an attribute certificate.

Paragraph at page 32, lines 22-30:

In response to receiving the request, the attribute certificate authority generates and signs attribute certificate **530** that contains encrypted authorization attributes **526**. Other fields of attribute certificate **530** would be filled with any appropriate or necessary data. Attribute certificate authority **529** then sends attribute certificate **530** to client SSO manager **510**, which stores the attribute certificate for later use, preferably within local secure user keystore **518**.

Marked-up set of paragraphs

The following section is a marked-up set of the current paragraphs as amended herein and as cleanly presented in the rewritten paragraphs provided above. The additions to the paragraphs are presented with double-underline and the deletions are presented using strike-through.

Paragraph at page 31, lines 5-20:

Continuing with the configuration phase, client SSO manager **510** uses the public key belonging to user **500** to obtain or generate an attribute certificate in the following manner. Client SSO manager **510** encrypts one or more sets of authentication data **512** with the public key of user **500**, thereby generating encrypted authorization attributes **526**. The encrypted authorization information is then placed into request **528** for requesting an attribute certificate, along with associated identifying information for user **500** and target legacy applications **502** as required by the format of the request and/or attribute certificate, and sent to attribute certificate authority 529~~520~~. In the preferred embodiment, the encrypted authorization information has been generated with an appropriate format so that attribute certificate authority 529~~520~~ can copy it into an attribute certificate.

Paragraph at page 32, lines 22-30:

In response to receiving the request, the attribute certificate authority generates and signs attribute certificate **530** that contains encrypted authorization attributes **526**. Other fields of attribute certificate **530** would be filled with any appropriate or necessary data. Attribute certificate authority 529~~520~~ then sends attribute certificate **530** to client SSO manager **510**, which stores the attribute certificate for later use, preferably within local secure user keystore **518**.

CONCLUSION

No new matter has been introduced by this amendment. For any other outstanding matters or issues, the examiner is urged to call or fax the below-listed telephone numbers to expedite the prosecution and examination of this application.

DATE: August 22, 2001

Respectfully submitted,

Joseph R. Burwell
Reg. No. 44,468
ATTORNEY FOR APPLICANT

Law Office of Joseph R. Burwell
P.O. Box 28022
Austin, Texas 78755
(512) 502-9448 (voice)
(512) 597-1218 (fax)